Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

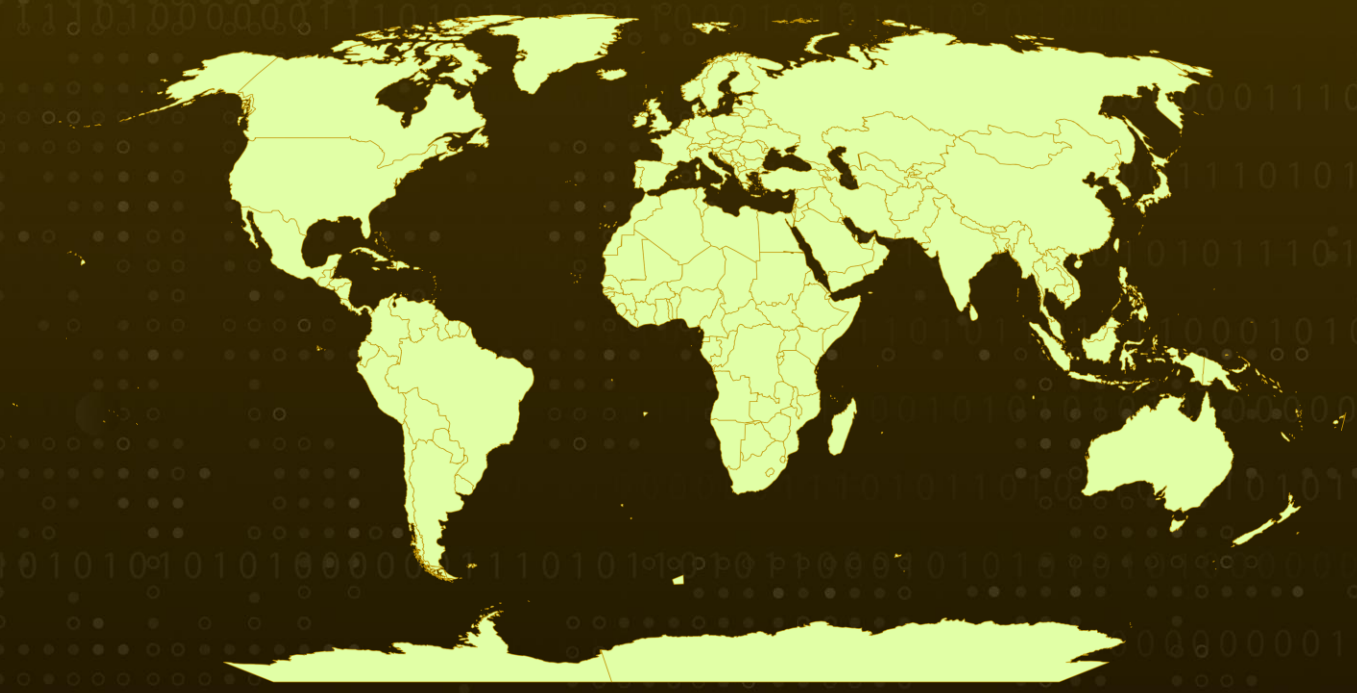
Titan Stealer: A Cross-Platform Information Stealer Malware Distributed by Threat Actors

Date of Publication	Admiralty Code	TA Number
January 26, 2023	A1	TA2023046

Summary

First appeared: 2022
Attack Region: Worldwide
Attack: Titan Stealer is a cross-platform information stealer malware actively distributed by a threat actor through a Telegram channel, capable of stealing various information from infected Windows machines and providing the attacker with access to victims' login activities and data.

Attack Regions



Attack Details

#1 Titan Stealer is a new malware that has been observed among threat actors, using Golang to create information stealer malware. The Titan Stealer panel includes a “Builder” page that allows threat actors (TA) to create a customized version of the stealer executable. This executable can be compiled with a user-specified build ID and file extensions to grab and gather sensitive information from the victim’s machine using the domain name.

#2 A campaign involving the Titan Stealer malware is being marketed and sold by a TA through a Telegram channel for cybercrime purposes. The stealer can steal a variety of information from infected Windows machines, including credential data from browsers and crypto wallets, FTP client details, screenshots, system information, and grabbed files.

#3 The malware attempts to read all the files in the "User Data" folder of various browsers using the CreateFile API, in order to steal information such as credentials, autofill states, browser metrics, crashpad data, crowd denies data, cache data, code cache data, extension state data, GPU cache data, local storage data, platform notifications data, session storage data, site characteristics database data, storage data, and sync data.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1055 Process Injection
T1055.012 Process Hollowing	T1083 File and Directory Discovery	T1082 System Information Discovery	T1041 Exfiltration Over C2 Channel
T1204 User Execution	T1003 OS Credential Dumping	T1552 Unsecured Credentials	T1518 Software Discovery
T1087 Account Discovery	T1005 Data from Local System	T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e7f46144892fe5bdef99bdf819d1b9a6 b10337ef60818440d1f4068625adfaa2 1af2037acbabfe804a522a5c4dd5a4ce 01e2a830989de3a870e4a2dac876487a 78601b24a38dd39749db81a3dcba52bd b0604627aa5e471352c0c32865177f7a 1dbe3fd4743f62425378b840315da3b7 5e79869f7f8ba836896082645e7ea797 2815dee54a6b81eb32c95d42afae25d2 cbe8e15c575d753324413f917ecbe245 6e090ecf5cc303cf305932c7998e8553 2bb3b6a9e445047087fe27ecb1cac2dc 82040e02a2c16b12957659e1356a5e19 a98e68c19c2bafe9e77d1c00f9aa7e2c 7f46e8449ca0e20bfd2b288ee6f4e0d1 d79252fc03409494c21963842bb880c7 b7729d9da4b68849baad56b115fcad79 00f0b502e17c9525e9e52ac8f524b525 b07263f74d432404b68c0bb1ad2f7844 0f3ac2b54489cfb63beffdec269c9f0e

TYPE	VALUE
SHA1	2155e10488f0e1bec472c6c80ab23271c94f18e8 5936d4e9771ff57ac41852eae6865418fe041e1f a51f8ce5cc8bf6c82bcec3caf1836059d729ebe0 f380628ad32e7a2b805e73802d9c33b3b19ccd23 94efe24e005bfb0158559978a7555800bc2a0415 9620f97ab57a8c274f661a70c96f546e6fd30f82 90097f106675b3ee460a9d32f94d15cb6f8daefe a4bc61e671875a5a63f3221b9e04d9295bc8e5be 4221774bb845ec56aa02b63dcb515f177fe31683 87c9bd18058ded5cc0d3e0d409a27c485a9dcc7a b5f00f28d9c7dd66df6d2151a6fb52d908504b10
SHA256	0e4800e38fb6389f00d9e35f1a65669fecb3abf141a2680b9b8a 5b5d255ae2cb 6e96dcad29a10b63f89f50040f107cdd29e850aa21c583134497 6953f6704ff5 28ed2fded652523af511803dbea91b8cefc040ecec703b5308a6 c849fb009888 32e1fafe04aa05424aaf18bca254760e87bba0114a16788a0676 8233ea9b70ab 129c9bdfe44b7b79abf04f56b35a65edd43d63b6294c7f05a3d1 40413533f385 421dbec55ce3481c5cecb630b4d216bacd07ce35a912abe57af8 1a3641414e83 4264a0c8d7acc6f10539285aa557a2d9d0298285b0a75a51a28 3241ccf11c94f a7dfb6bb7ca1c8271570ddcf81bb921cf4f222e6e190e5f420d4 e1eda0a0c1f2 dd3730841bb62b131a08cb37fbd8e1e541fb9cab6baf6c378e84 d1c77e858e3a e4584bb5db986d9f64297863cd5a7c4062aeeb7e4775dbda4d9 3d760406165a8 e01264912f6b5d3f3cd84261b4b19408c317e06f83292d6f2ca8 7ebfb0b71fdc
URLs	http[:]//77.73.133.88[:]5000 http[:]//77.73.133.88[:]5000/sendlog

References

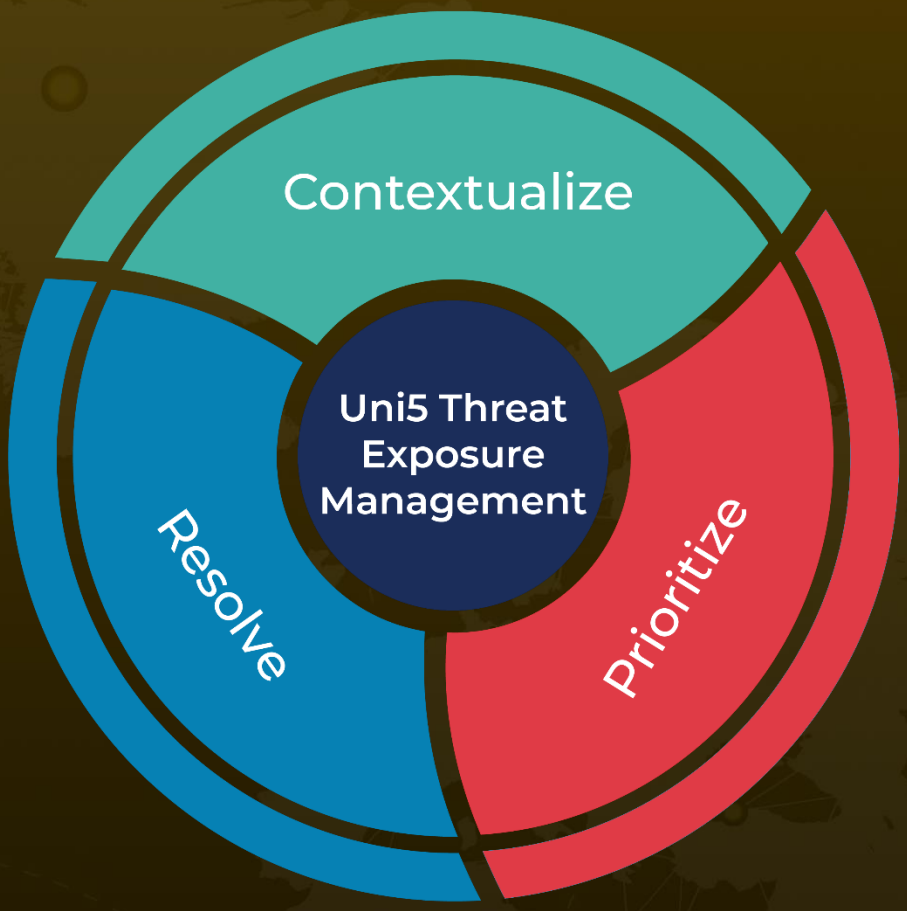
https://www.uptycs.com/blog/titan-stealer-telegram-malware-campaign

https://blog.cyble.com/2023/01/25/titan-stealer-the-growing-use-of-golang-among-threat-actors/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 26, 2023 . 2:45 AM

More at www.hivepro.com